Measurement-device-independent Quantum Key Distribution (MDI-QKD)

• Imperfections in real-world QKD systems can create security loopholes.
• In MDI-QKD, the users (Alice and Bob) send their signals to Charlie, who interferes them.
• The measurement results only reveal the correlation between Alice and Bob’s bits, but not the bit values, this allows MDI-QKD to remove all detector loopholes.

Experimental Setup

Bit encoding with directly modulated lasers

• Z-basis: modulate the electrical driving signal of the secondary laser, selectively switching the laser on in the desired time bin.

• X-basis: modulate the electrical driving signal of the primary laser, the perturbation signal changes the phase evolution of the primary pulses, which imposes a phase difference on the secondary pulses through laser seeding.

Secure key rates

• QBERs as low as 0.55% are recorded in the Z basis and as low as 26.6% in the X basis, showing the practicality of the technique.
• Our design improves the state-of-the-art key rates by about an order of magnitude, up to 8 bps at 54 dB (equivalent to 340 km fiber).

References: